Chap 3 Adressage

3.1. Introduction

Il existe plusieurs types d'adresses qui doivent être incluses pour livrer correctement les données depuis une application source exécutée sur un hôte à l'application de destination correcte exécutée sur un autre dans le modèle OSI : des adresses MAC ou adresses physiques à la couche liaison de données, des adresses IP ou adresses logiques à la couche réseau, un numéro de port au niveau de la couche Transport pour identifier un processus client ou serveur de la couche Application, chaque protocole de la couche Application peut posséder un adressage particulier associé à son service. On peut citer par exemple l'adressage par URL pour le service WEB ou l'adressage par email pour le service messagerie.

3.2. Adressage physique

L'adressage physique utilise une adresse matérielle (appelée généralement MAC) qui permet d'identifier de manière unique l'interface de communication d'un équipement sur un réseau physique. Une adresse MAC est un identifiant unique attribué à chaque carte réseau. Concrètement, c'est un numéro d'identification composé de 12 chiffres hexadécimaux. Par convention, on place un symbole deux-points (:) tous les 2 chiffres. Exemple **01:23:45:67:89:AB**.

Les adresses MAC :

- Sont utilisées dans les entêtes des trames de la couche Liaison afin d'identifier l'émetteur et le destinataire.
- Sont codées sur 48 bits soit 6 octets (les trois 3 premiers octets permettent d'identifier le fabricant de l'interface de communication).
- Ne donnent aucune indication sur la situation "géographique" de l'équipement et donc ne permet pas une organisation optimale du réseau. Cette faiblesse sera compensée par un adressage logique au niveau de la couche Réseau.

3.3. Adressage logique

L'adressage logique ou adressage IP intervient au niveau de la couche réseau afin d'identifier un équipement dans un réseau. Les adresses IP sont utilisées dans les entêtes des paquets afin d'identifier l'émetteur et le destinataire. Elles sont codées sur 32 bits (pour la version 4 : IPv4) et sur 128 bits (pour la version 6 : IPv6). Les adresses IP sont le seul moyen d'identification des machines sur Internet. Chaque version utilise sa propre structure d'adresse IP.
Une "adresse IPv4" est constituée de 4 nombres correspondant à **4 octets** compris entre 0 et 255, séparés par des points. **Exemple** : 192.145.24.1.
Les "adresses IPv6" sont encore plus complexes : elles sont représentées par une suite de 8 groupes de 2 octets représentés en hexadécimal **Exemple** 1fff:0000:0a88:85a3:0000:0000:ac1f:8001.

3.3.1. Techniques d'adressage

On distingue différentes techniques d'adressage :

- L'unicast désigne une adresse réseau unique permettant d'identifier un hôte sur un réseau.
- Le broadcast permet le transfert d'un hôte vers tous les autres hôtes, en utilisant une adresse spécifique nommée adresse de broadcast (ou adresse de diffusion générale).
- Le multicast permet la communication simultanée avec un groupe d'ordinateurs identifiés par une adresse spécifique nommée adresse de multicast (ou adresse de groupe). Les récepteurs intéressés par les messages adressés en multicast doivent s'abonner au préalable à ce groupe.
- L'anycast désigne une technique où on l'on dispose de plusieurs adresses pour une destination mais une seule sera utilisée.

3.3.2. Affectation des adresses IP

On distingue 2 méthodes d'attribution d'adresses IP pour les hôtes :

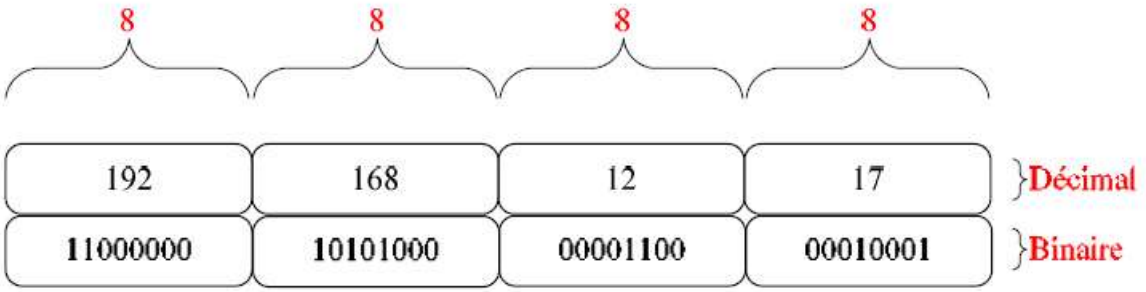
- **Statique** : chaque équipement est configuré manuellement avec une adresse unique
- **Dynamique** : On utilise des protocoles qui attribuent des IP aux hôtes
    - **RARP (Reverse Address Resolution Protocol)** : Protocole associant les adresses MAC aux adresses IP. Il permet à des stations sans disque dur local connaissant leur adresse MAC de se voir attribuer une IP.
    - **BOOTP (Bootrap Protocol)** : Ce protocole permet à un équipement de récupérer son adresse IP au démarrage. L'émetteur envoie un message de broadcast (255.255.255.255) reçu par le serveur qui répond lui aussi par un broadcast contenant l'adresse MAC de l'émetteur ainsi qu'une IP.
    - **DHCP (Dynamic Host Configuration Protocol)** : Remplaçant de BOOTP, il permet l'obtention dynamique d'IP. Lorsqu'un ordinateur entre en ligne, il communique avec le serveur qui choisit une adresse et un masque de sous réseau et l'attribue à l'hôte. Il permet de plus d'obtenir des serveurs DNS, la passerelle par défaut ainsi qu'optionnellement les adresses des serveurs WINS.

3.3.3. Passerelle par défaut

La passerelle, également appelée passerelle par défaut, est requise pour envoyer un paquet en dehors du réseau local.

3.3.4. Adresse IPv4

Une adresse IPv4 est une séquence de 32 bits composée de 1 et de 0. Afin de faciliter leur lecture, les adresses IPv4 sont généralement exprimées sous la forme de quatre nombres décimaux (4 octets) compris entre 0 et 255, séparés par des points. Par exemple, l'adresse IP 192.168.1.8 correspond à la valeur 11000000.10101000.00000001.00001000 en notation binaire.



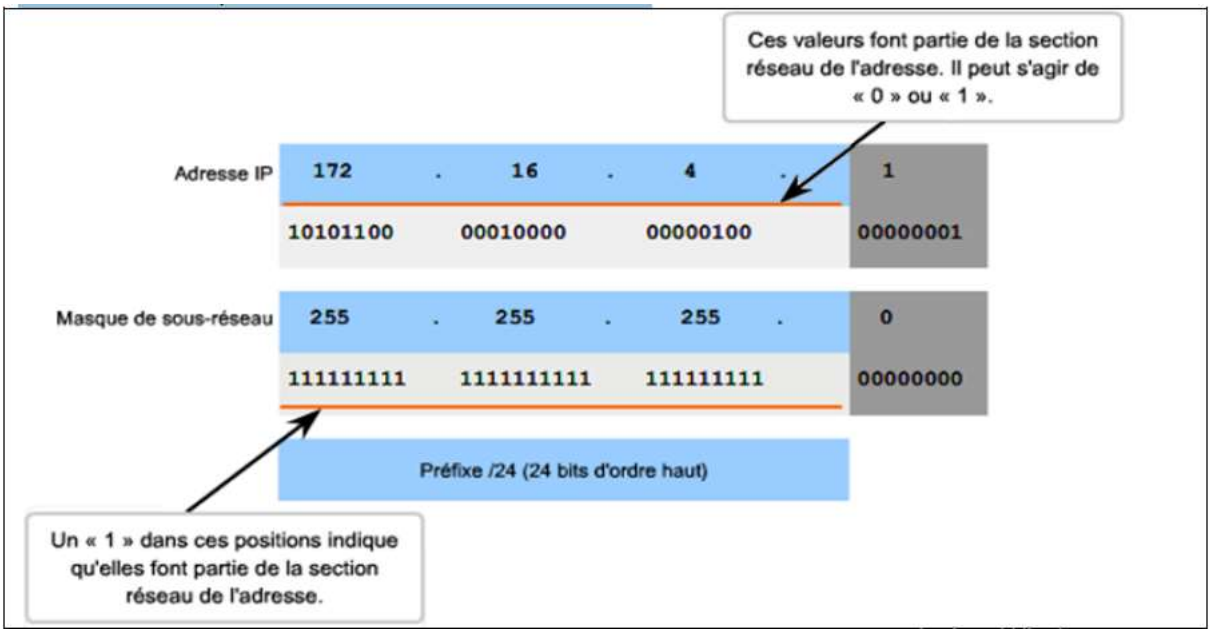
Exemple d'adresse IP

3.3.4.1. Masque de sous-réseau

Pour définir les parties réseau et hôte d'une adresse, les périphériques utilisent une configuration de 32 bits appelée « masque de sous-réseau ». Le masque de sous-réseau s'exprime dans le même format décimal pointé que celui de l'adresse IPv4. Le masque de sous-réseau est créé en plaçant le nombre binaire 1 dans chaque position de bit qui représente la partie réseau et en plaçant le nombre binaire 0 dans chaque position de bit qui représente la partie hôte.

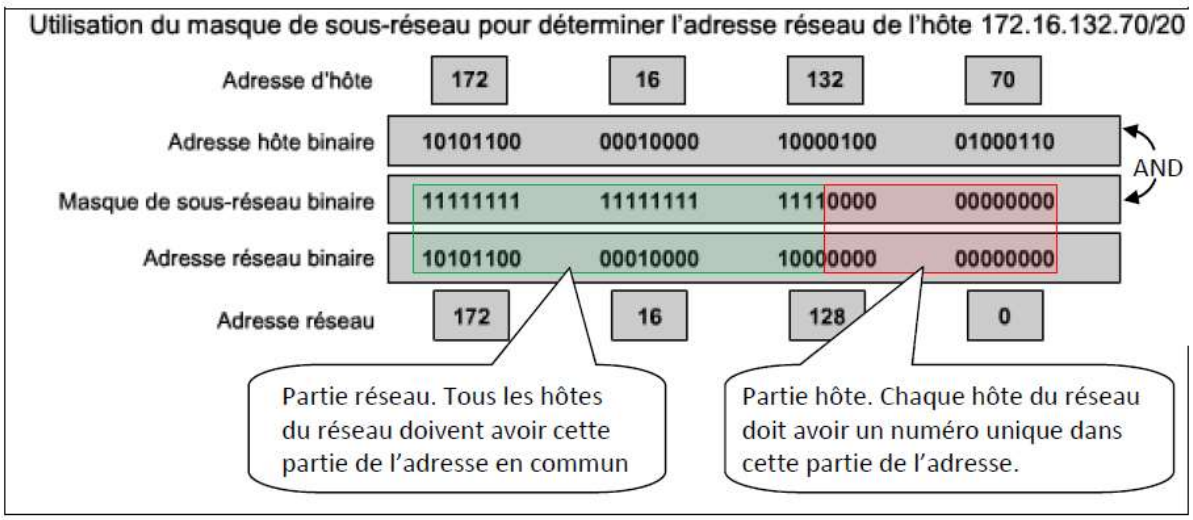
Le masque de sous-réseau est aussi appelé « préfixe ». Ce dernier un nombre de 0 à 32 qui représente le nombre de bits à 1 dans le masque de sous-réseau. Il représente la même chose : la partie réseau d'une adresse.

Par exemple, le préfixe /24, correspondant au masque de sous-réseau 255.255.255.0 (11111111.11111111.11111111.00000000). Les bits restants (à droite) du masque de sous-réseau sont des zéros, et indiquent l'adresse de l'hôte sur le réseau.



Exemple : Déterminer l'adresse de réseau de l'hôte 172.16.132.70/20

Pour déterminer l'adresse du réseau auquel appartient un hôte, on effectue le masquage de son adresse IP par son masque de sous-réseau. Le masquage est obtenu en effectuant une opération AND bit à bit entre les deux adresses :



Conclusion : L'hôte **172.16.132.70/20** fait partie du réseau **172.16.128.0/20**
Ce réseau a les caractéristiques suivantes :

3.3.4.2. Réseaux et hôtes

La principale fonction de l'IP, dont les initiales signifient « protocole Internet », est de permettre l'établissement des communications entre des réseaux. C'est pourquoi une adresse IP est composée de deux parties :

- L'identifiant de réseau (netid ou ID de réseau ou adresse du réseau) spécifie le réseau sur lequel un ordinateur hôte peut être trouvé.
- L'identifiant d'hôte (hostid ou ID d'hôte ou adresse de l'hôte) spécifie un périphérique présent sur le réseau selon son identifiant de réseau.

3.3.4.3. Décimales pointées

Une adresse IP est usuellement représentée sous une forme appelée *notation décimale pointée*. Grâce à cette notation, chaque groupe de huit bits, appelé *octet*, est représenté par son équivalent décimal. Prenons par exemple cette adresse IP :
11000000101010001000100000011100
L'équivalent en notation décimale pointée est :
192.168.136.28

3.3.4.4. Systèmes d'adressage

Il existe en réseau deux systèmes d'adressage : l'adressage par classes et l'adressage CIDR (sans classes).
L'adressage par classes est un système utilisant une architecture réseau appelée en anglais classful network, c'est-à-dire « réseau dans les classes ».
Le système d'adressage par classes fonctionne selon le principe suivant : les adresses IP sont rangées par classes et dans chacune d'elles se trouvent des plages. Si une entreprise demandait des adresses pour cent ordinateurs, on choisirait la classe lui offrant ce nombre d'adresses et on lui offrirait des adresses IP issues de cette classe.
L'adressage sans classes (ou adressage CIDR) est le système de gestion et d'allocation d'adresses IP le plus utilisé aujourd'hui.

3.3.4.4.1. L'adressage par classe

Pour voir votre adresse IP sous Windows :

1. Cliquez sur Démarrer ;

2. Tous les programmes ;

3. Accessoires ;

4. Invite de commandes.

Dans l'invite de commandes, tapez **ipconfig.**

Une classe d'adresse IP est un ensemble d'adresses. Chaque adresse IP appartient à une classe principale (on dit aussi une plage). Chaque classe a un masque de sous-réseau par défaut.

À l'origine, la spécification RFC1700 regroupait les plages d'adresses en classes appelées classe A, B et C. Elle a également établi des adresses de classe D (multicast) et de classe E (expérimentales).

Classe A

Les adresses IP de la classe A se situent entre 1.0.0.0 et 127.255.255.255. Elles utilisent un préfixe /8 invariable, le premier octet indiquant l'adresse réseau. Les trois octets restants correspondent aux adresses d'hôte. Le bloc d'adresses de la classe A se situe entre 0.0.0.0 /8 et 127.0.0.0 /8. Son masque de sous-réseau par défaut est 255.0.0.0. Les adresses IP commençant par 127 sont utilisées pour faire des tests particuliers. Exemple d'adresse de classe A : 110.0.0.1.

Sous Windows, tapez : ping 127.0.0.1

Ou sous Linux, tapez : ping -c 4 127.0.0.1

Si le protocole TCP/IP est correctement implémenté, c'est à dire si votre système d'exploitation est capable de se connecter à un réseau, vous aurez une suite de réponses de votre carte réseau, généralement 4 lignes.

On appelle l'adresse 127.0.0.1 l'appelle loopback address. Le mot loopback signifie "boucle de retour". Donc, lorsque vous faites ping 127.0.0.1, vous faites en réalité un ping vers... votre ordinateur. En fait, votre système d'exploitation crée automatiquement un réseau spécial composé uniquement de lui-même. Sous Linux, ce réseau spécial est représenté par l'interface lo. Cela permet de tester des applications réseau sans être connecté réellement à un réseau.

Classe B

Les adresses IP de la classe B sont celles entre 128.0.0.0 et 191.255.255.255. Elles utilisent un préfixe /16 invariable, les deux premiers octets indiquant l'adresse réseau. Les deux octets restants correspondent aux adresses d'hôte. Le bloc d'adresses de la classe B se situe entre 128.0.0.0 /16 et 191.255.0.0 /16. Le masque de sous-réseau de la classe B par défaut est 255.255.0.0. Exemple d'adresse de classe B : 134.157.0.1

Classe C

Les adresses de la classe C sont entre 192.0.0.0 et 223.255.255.255. Elles utilisent un préfixe /24 invariable, les trois premiers octets indiquant l'adresse réseau. L'octet restant correspondait aux adresses d'hôte. Le bloc d'adresses de la classe C se situe entre 192.0.0.0 /24 et 223.255.255.0 /24. Le masque de sous-réseau de la classe C par défaut est 255.255.255.0. Exemple d'adresse de classe C : 192.70.89.1

Classes D et E

Ce sont des classes expérimentales.
Classe D : de 224.0.0.0 à 239.255.255.255 ;
Classe E : de 240.0.0.0 jusqu'à 255.255.255.255.

Classe	Plage d'adresse	Longueur adresse réseau	Nombre de réseaux	Nombre maximal de machines
A	1.0.0.0 – 127.255.255.255	1 octet	127	16777216
B	128.0.0.0 – 191.255.255.255	2 octets	16384	65536
C	192.0.0.0 – 223.255.255.255	3 octets	2097152	256
D	224.0.0.0 - 239.255.255.255			
E	240.0.0.0 - 255.255.255.255			

L'organisme chargé d'attribuer les adresses IP publiques est l'InterNIC (Internet Network Information Center). Le premier bit d'une adresse de classe A est toujours 0. Une adresse de classe C commence par la valeur binaire 10. Les trois premiers bits du premier octet d'une adresse de classe B sont toujours 110. Les quatre premiers bits d'une adresse de classe D doivent correspondre à 1110. Les quatre premiers bits d'une adresse de classe E sont toujours des 1.

Plages d'adresse IPv4 exclues de l'adressage des hôtes

- **Adresses réseau et de diffusion**

La première et la dernière adresse ne peuvent pas être attribuées à des hôtes. Il s'agit respectivement de l'adresse réseau et de l'adresse de diffusion.

- **Route par défaut**

La route IPv4 par défaut est représentée de la manière suivante : 0.0.0.0. La route par défaut est utilisée comme route « dernier recours » lorsqu'aucune route plus spécifique n'est disponible. L'utilisation de cette adresse réserve également toutes les adresses de la plage 0.0.0.0 - 0.255.255.255 (0.0.0.0 /8).

- **Bouclage**

L'adresse de bouclage IPv4 127.0.0.1 est une autre adresse réservée.

- **Adresses locales-liens**

Les adresses IPv4 du bloc d'adresses 169.254.0.0 à 169.254.255.255 (169.254.0.0 /16) sont conçues pour être des adresses locales-liens. Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation, dans les environnements où aucune configuration IP n'est disponible. Celles-ci peuvent être utilisées dans un réseau Peer to peer de petite taille ou pour un hôte qui ne peut pas obtenir d'adresse automatiquement auprès d'un serveur DHCP.

- **Les adresses de multidiffusion (multicast)**

Les adresses de multidiffusion IPv4 du bloc 224.0.0.0 - 224.0.0.255 sont des adresses de liaison locales réservées. Ces adresses s'appliquent aux groupes de multidiffusion d'un réseau local.

- **Les adresses expérimentales**

La plage d'adresses expérimentales IPv4 s'étend de 240.0.0.0 à 255.255.255.254.

- **Les adresses publiques**

Les adresses publiques sont routables sur internet et ne peuvent par conséquent pas être utilisées sur un réseau privé. Ces adresses étaient à l'origine réparties sur les trois classes de monodiffusion (unicast) (A, B et C).

Remarque Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI) ou d'un registre moyennant une participation. Les adresses IP privées constituent une solution au problème de pénurie des adresses IP publiques. Le routage CIDR (Classless interdomain routing) et la norme IPv6, ont été développé également pour résoudre ce problème.

Notion de classe privée

Une classe privée est une portée d'adresses IP d'une certaine classe publique (A, B, C), mais réservée pour un usage particulier par des standards ou conventions

Plages d'adresses privées :

Classe	Plages d'adresses

A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

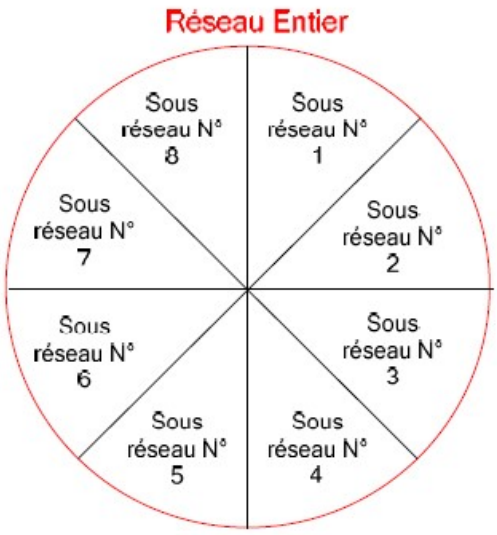
La connexion d'un réseau à Internet par le biais d'adresses publiques nécessite la conversion des adresses privées en adresses publiques. Ce processus de conversion est appelé « NAT » (*Network Address Translation*). L'équipement chargé d'exécuter le système NAT est généralement un routeur.

Le Subnetting

Le subnetting est une technique qui consiste à diviser un réseau plus large en plusieurs sous-réseaux. Le subnetting est l'action de créer des sous-réseaux en personnalisant les masques.

Intérêt du découpage réseau

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée a consisté à découper une classe d'adresses IP A, B ou C en sous-réseaux. Cette technique est appelée « subnetting ». Le découpage en sous-réseaux ou sous-réseautage est une technique qui permet à l'administrateur réseau d'utiliser plus efficacement les 32 bits d'une adresse Internet afin de créer des réseaux capables de s'affranchir des limites imposées par les adresses IP de classes A, B et C. Il est ainsi possible de créer des réseaux dont le nombre d'hôtes est mieux adapté aux besoins.



Pour cela, on emprunte à la partie hôte des bits que l'on désigne comme champ de sous réseaux. Le nombre minimal de bits à emprunter est de 2 et le nombre maximal est égal à tout nombre laissant 2 bits à la partie hôte.

Il faut savoir qu'il y a une perte d'adresses quand on utilise le mécanisme de création de sous réseaux :

- Tout d'abord au niveau des sous réseaux eux-mêmes, le premier sous réseau et le dernier doivent être enlevés. En effet, La première adresse sera l'adresse de réseau : ce sera l'adresse réseau pour la globalité du réseau. La dernière plage ayant l'adresse de

broadcast pour le réseau tout entier. Il faut donc enlever les deux plages entières pour éviter toute confusion. On aura donc N-2 sous réseaux utilisables.

- Pour les hôtes également, il y a une perte d'adresses, sans faire de sous réseaux, on avait une seule adresse réseau et une seule adresse broadcast, avec les sous réseaux, on va avoir une adresse de sous réseau à chaque sous réseau et une adresse de broadcast de sous réseau à chaque sous réseau. Il faut donc également penser à la règle des N-2 pour les hôtes.

Avantages du subnetting

- **Délégation de l'administration :** Le subnetting permettant de diviser un grand réseau en plusieurs réseaux plus petits, il permet de décentraliser l'administration, et éventuellement de déléguer la gestion de chaque sous-réseau à une personne différente. Dans une entreprise possédant un réseau de 1000 machines, sa gestion sera simplifiée.
- **La réduction du trafic :** Si 2 ordinateurs se trouvant dans un même sous-réseau communiquent, ils n'exploiteront que la bande passante allouée à leur sous-réseau, et non celle du réseau entier. Considérons une entreprise possédant un réseau de 500 machines. Il est divisé en 25 sous-réseaux de 20 machines. Ainsi, les machines appartenant à un même sous-réseau communiquant entre elles n'utilisent que la bande passante qui est allouée à leur sous-réseau, ce qui permet de ne pas réduire le débit des autres. Cela se remarque notamment lors du broadcast de données : elles ne sont transmises qu'aux ordinateurs du sous-réseau, et pas aux autres qui n'en ont probablement rien à faire. Le broadcast est utilisé notamment par le protocole ARP qui permet d'associer adresses MAC et adresses IP. Nous aurons peut-être l'occasion de traiter ce sujet en annexes.
- **La facilité du diagnostic :** Si par exemple un ordinateur consomme une quantité de bande passante inhabituelle, il est beaucoup plus aisé d'analyser son comportement pour régler le problème lorsqu'il se trouve dans un petit sous-réseau que lorsqu'il se trouve dans le même réseau que 1000 autres machines.
- **L'économie d'adresses :** Prenons par exemple une adresse IP : 200.10.0.5. Le masque de sous réseau par défaut est 255.255.255.0. Dans ce cas, on peut avoir jusqu'à 254 terminaux (clients) dans ce même réseau, donc 254 adresses IP. Ce qui veut dire que si vous avez un réseau de 10 ordinateurs, vous avez quand même 254 adresses IP disponibles. Mais comme vous ne les utilisez pas, vous les gaspillez. Toutefois, le subnetting ne nous permet pas d'économiser comme on le souhaite. Mais cela peut être utile pour des raisons de sécurité, entre autres.

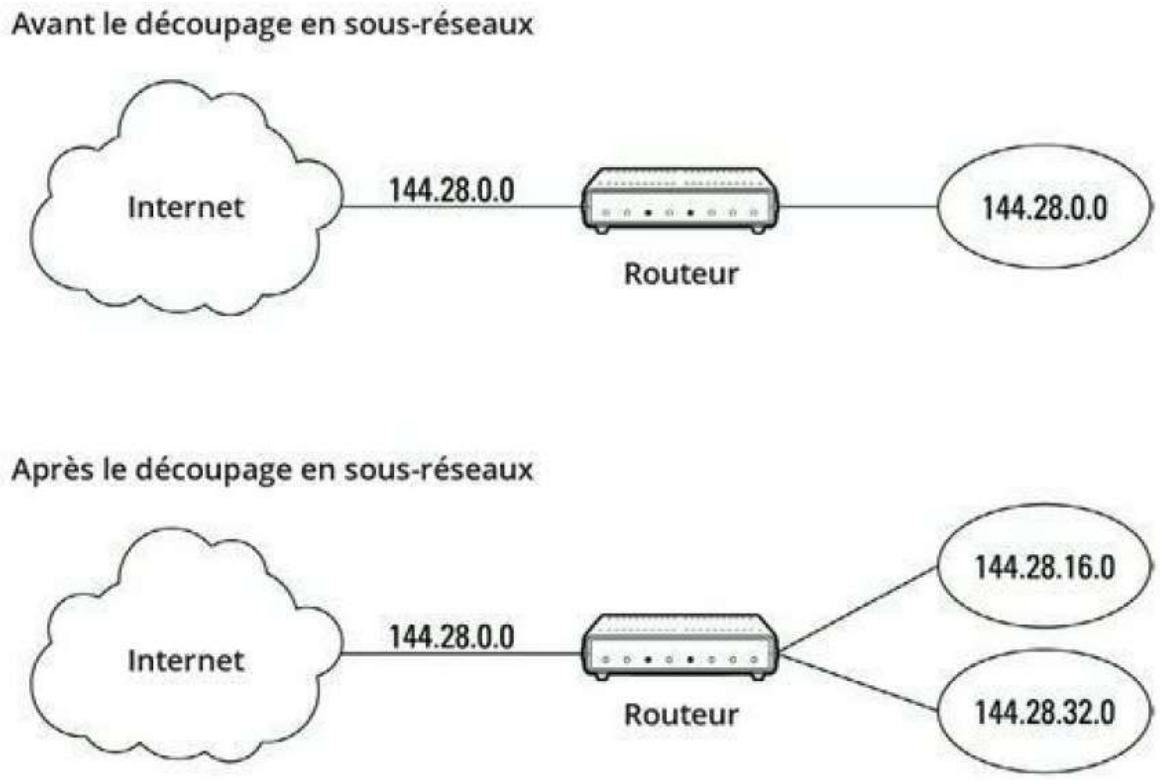
Sous-réseaux

On utilise les sous-réseaux pour les raisons suivantes :

- Utilisation hétérogène de moyens de couche 1,
- Réduction de l'encombrement,
- Economise les temps de calculs,
- Isolation d'un réseau,
- Renforcement de la sécurité,
- Optimisation de l'espace réservé à une adresse IP.

Nombre de sous réseaux : $2^n - 2$, n étant le nombre de bits à 1
On obtient ainsi les adresses des sous réseaux
Adresse de diffusion : Mettre tous les bits de la partie hôte à 1
Nombre de machines du sous réseau : $2^m - 2$, m étant le nombre de bits de la partie hôte

Un *sous-réseau* est un réseau qui fait partie d'un autre réseau (de classe A, B ou C). Les sous-réseaux sont créés en utilisant un ou plusieurs bits d'un hôte de classe A, B ou C pour étendre l'identifiant de réseau. Par conséquent, plutôt que d'avoir un identifiant de réseau standard de 8, 16 ou 24 bits, un sous-réseau peut avoir un identifiant de n'importe quelle longueur.
La figure suivante montre un exemple de réseau avant et après le découpage en sous-réseaux. Dans le réseau découpé, le réseau a reçu l'adresse de classe B 144.28.0.0. Tous les périphériques de ce réseau doivent partager le même domaine de diffusion.



Présentation d'un réseau avant et après son découpage en sous-réseaux.

Dans le second réseau, les quatre premiers bits de l'identifiant d'hôte sont utilisés pour diviser le réseau en deux petits réseaux, identifiés comme sous-réseaux 16 et 32. Dans le monde extérieur, c'est-à-dire de l'autre côté du routeur, ces deux réseaux apparaissent comme un seul réseau identifié par l'adresse IP 144.28.0.0. Par exemple, pour le monde extérieur, le périphérique à l'adresse 144.28.16.22 appartient au réseau 144.28.0.0. Par conséquent, un paquet envoyé à ce périphérique sera délivré au routeur avec l'adresse 144.28.0.0. Le routeur considère ensuite la partie sous-réseau de l'identifiant d'hôte pour décider d'acheminer le paquet vers le sous-réseau 16 ou vers le sous-réseau 32.

Méthodes de calcul

a) Méthode classique

On entend par méthode classique le fait de procéder sans formule spécifique, par la méthode calculatoire.

Cette méthode se détaille en 6 étapes :

- Empruntez le nombre de bits suffisants
- Calculez le nouveau masque de sous réseau
- Identifiez les différentes plages d'adresses IP
- Identifiez les plages d'adresses non utilisables
- Identifiez les adresses de réseau et de broadcast
- Déterminez les plages d'adresses utilisables pour les hôtes.

- **Empruntez le nombre de bits suffisant**

Il faut tout d'abord déterminer le nombre de bits que l'on va emprunter à la partie réseau. On détermine tout d'abord le nombre d'hôtes ou de sous réseaux maximums que l'on désire, car suivant ce nombre, on n'utilisera pas les même plages d'adresses (254 hôtes maximum pour une plage de classe C, 65534 pour une plage de classe B et 16 777 216 pour une plage de classe A) On écrit en binaire le chiffre souhaité de sous-réseaux ou d'hôtes ce qui nous donne le nombre de bits à emprunter ou à laisser. Il faut penser à la règle des N-2, on cherche des plages utilisables. Il faut donc penser à additionner 2 aux hôtes ou aux sous réseaux utilisables que l'on cherche à avoir.
Pour les sous réseaux nous allons emprunter des bits à la partie hôte (allonger le masque) et pour les hôtes nous allons laisser les bits à 0 pour le nombre d'hôtes souhaités.

- **Calculez le nouveau masque de sous réseau**

Maintenant que l'on sait combien de bits l'on va emprunter, on calcule le nouveau masque de sous réseau auquel on emprunte les bits à la partie hôte. Pour cela on prend le masque de la plage que l'on veut utiliser, on le convertit en binaire, puis on emprunte le nombre de bits nécessaires à 1 pour la création des sous réseaux.
Ou bien on laisse le nombre suffisant de bits à 0 pour les hôtes.

- **Identifiez les différentes plages d'adresses**

A l'aide du masque de sous réseau on calcule les différentes plages d'adresses possibles. Pour cela il suffit d'écrire chaque possibilité binaire sur les bits que l'on a empruntés pour la création des sous réseaux.

- **Identifiez les plages d'adresses non utilisables**

On retire maintenant la première et la dernière plage d'adresse des différents choix que l'on a. La première adresse sera l'adresse de réseau : ce sera l'adresse réseau pour la globalité du réseau. La dernière plage ayant l'adresse de broadcast pour le réseau tout entier.

- **Identifiez les plages de réseau et de broadcast**

Des plages d'adresses qui restent, on retire aussi les premières et dernières adresses. La première servira d'adresse réseau pour la plage d'adresse. La dernière servira d'adresse de broadcast pour la plage spécifiée.

- **Déterminez les plages d'adresses Hôtes.**

Maintenant qu'il ne nous reste plus que les plages d'adresses utilisables, on a donc les plages d'adresses IP utilisables par les hôtes pour communiquer sur le sous réseau.

b) Méthode du nombre magique

Cette méthode permet d'aller plus vite dans le calcul, elle est basée sur la formule que voici :

256 = Masque de sous réseau + Taille du sous réseau

Cette formule va vous permettre de calculer rapidement :

- Un masque de sous réseau
- Un nombre d'hôtes par sous réseau

Cette formule est propre à l'octet modifié avec le masque de sous réseau.
Elle permet de trouver le nombre d'hôtes par sous réseaux très vite, dès que l'on a le masque.
Il suffit de soustraire au nombre magique la valeur de l'octet du masque modifié, le résultat ainsi donné est la taille du sous réseau par rapport à cet octet.

Exemple :
On vient de faire du Subnetting sur une classe C, on a donc un masque résultant en 255.255.255.224.
On applique le nombre magique, 256-224=32, il va donc y avoir 32 hôtes par sous réseau (30 utilisables).
On peut également extrapoler, et ce résultat indique donc que les plages de sous réseau seront espacées de 32.

En annexe, on peut également utiliser une formule logique afin de simplifier la création de sous réseaux :
256 = Taille du sous réseau * Nombre de sous Réseaux

Exemple :
On désire savoir le nombre d'hôtes sur 5 sous réseaux avec une classe C on aura donc un masque de type 255.255.255.X
La puissance de 2 la plus proche et supérieur à 5 est donc 8.

On prend la formule :
256 = Taille du sous réseau * Nombre de sous Réseau
Et on l'applique :
256 = Taille du sous réseau * 8
Taille du sous réseau = 256/8 = 32
En enlevant les 2 adresses (celle du sous réseau et celle de broadcast) on a un total de 30 adresses utilisables par sous réseau.

Exercice d'application

Pour configurer l'interface d'un hôte qui doit se connecter à un réseau existant, on nous donne l'adresse 172.16.19.40/21.

1) Quel est le masque réseau de cette adresse ?
2) Combien de bits ont été réservés pour les sous-réseaux privés ?
3) Combien de sous-réseaux privés sont disponibles ?
4) Quelle est l'adresse du sous-réseau de l'exemple ?
5) Quelle est l'adresse de diffusion du sous-réseau de l'exemple ?

3.3.4.4.2. L'adressage CIDR et supernetting

Le système CIDR a été conçu pour remplacer l'adressage par classes.
Le but de ce nouveau système s'articule autour de deux points :

- Économiser les adresses IP.
- Faciliter le routage.

CIDR : comment
Soit l'adresse 192.168.10.0/23.
À ce stade, vous êtes censés savoir que le nombre après le slash (/) équivaut au nombre de bits masqués. 192.168.10.0/23 applique un masque de 255.255.254.0 au réseau 192.168.10.0.
Grâce à cette notation, nous pouvons calculer (et vous êtes censés savoir le faire seuls à présent) l'étendue du sous-réseau qui ira donc de 192.168.10.0 à 192.168.11.255 (si nous incluons l'adresse de diffusion ou broadcast address), dans un réseau sans classes.
Par contre, si nous étions dans un réseau n'utilisant pas l'adressage CIDR, 192.168.10.0/23 représenterait une fusion de deux sous réseaux de la classe C, 192.168.10.0 et 192.168.11.0 ayant chacun un masque de sous-réseau de…255.255.255.0.
Cela dit, avec l'adressage CIDR, le masque /23 nous donne l'équation suivante :
192.168.10.0/23 (adressage CIDR) = 192.168.10.0/24 (ou 255.255.255.0) + 192.168.11.0/24 (ou 255.255.255.0)
Nous avons la possibilité d'utiliser un seul réseau qui fusionne plusieurs sous-réseaux. Cette fusion de sous-réseaux, dite aussi supernetting, est l'essence même de CIDR. Cette technique est également appelée résumé de routes (route summarization en anglais).
Pour implémenter un réseau fondé sur l'adressage CIDR, il faut utiliser un protocole qui puisse le supporter. Il en existe plusieurs, tels que BGP et OSPF. En général, les petits LAN et les réseaux « maison » n'implémentent pas l'adressage CIDR.

Comment résumer une route
Si nous avons quatre subnets tels que :
Subnet 1 : 192.168.0.0/24 soit 11000000. 10101000. 00000000.00000000/24
Subnet 2 : 192.168.1.0/24 soit 11000000. 10101000. 00000001.00000000/24
Subnet 3 : 192.168.2.0/24 soit 11000000. 10101000. 00000010.00000000/24
Subnet 4 : 192.168.3.0/24 soit 11000000. 10101000. 00000011.00000000/24

Nous remarquons que ces quatre subnets ont bien le même préfixe /24 : nous pouvons les fusionner sous un seul préfixe. Par conséquent, nous obtenons la route suivante : 192.168.0.0/22 soit 11000000.10101000.00000000.00000000/22.

Pour obtenir le /22, nous avons suivi quatre étapes bien précises que vous devez suivre également.

Étape 1 : détecter les réseaux ayant le même préfixe
Dans cette étape, nous avons pris quatre réseaux ayant le même préfixe (/24) : il s'agit de 192.168.0.0, 192.168.1.0, 192.168.2.0 et 192.168.3.0.

Étape 2 : convertir des réseaux en binaire

Ensuite, nous avons converti chaque adresse réseau en binaire. Pourquoi ? Parce que c'est important pour l'étape 3.

Étapes 3 et 4 : détecter les motifs entre les sous-réseaux en binaire (étape 3) et les compter (étape 4)
Quand nous avons converti les quatre sous-réseaux en binaire, qu'avons-nous obtenu ?

Subnet 1 : 11000000. 10101000. 00000000. 00000000
Subnet 2 : 11000000. 10101000. 00000001. 00000000
Subnet 3 : 11000000. 10101000. 00000010. 00000000
Subnet 4 : 11000000. 10101000. 00000011. 00000000

Y a-t-il quelque chose de commun à ces quatre sous-réseaux ?
Tous ces sous-réseaux ont 11000000.10101000.000000 en commun. Comptons le nombre de bits : il y en a 22. 22 sera donc notre nouveau préfixe. Le network ID sera la plus petite adresse IP parmi les quatre, soit 192.168.0.0. Enfin, la nouvelle route, la route résumée ou agrégée, sera 192.168.0.0 /22.

CIDR facilite l'écriture des tables de routage.

3.4. Adressage IPv6

Contrairement aux adresses IPv4, les adresses IPv6 s'écrivent en hexadécimal et non en décimal. En IPv6, il y a 8 nombres hexadécimaux inférieurs à FFFF séparés par le symbole « : », cela prend 16 octets (128 bits).
Dans une adresse IPv6, « :: » signifie « remplir avec autant de zéros qu'il faut pour avoir 128 bits».

L'adresse privée de sortie
"adresse de liaison locale" commence forcément par FE80::/10.
FE80(16) = 1111 1110 1000 0000(2)
Cela signifie que les 10 premiers bits d'une adresse de lien local valent obligatoirement 1111111010.
Voici donc quelques exemples d'adresses de lien local :
FE80::1 (1111 1110 1000 0000 [111 zéros] 1)
FE85::2:1:dada (1111 1110 1000 0101 [78 zéros] 10 0000 0000 0000 0001 1101 1010 1101 1010)
FE93::3 (1111 1110 1001 0011 [110 zéros] 11)
La particularité de cette adresse est qu'elle ne peut être utilisée que pour contacter un hôte directement connecté.

Pour obtenir une adresse IPv6, il y a plusieurs manières. Soit il y a un serveur DHCPv6 qui distribue des adresses à tour de bras sur le réseau et on prend ce qu'il donne. Soit il n'y en a pas et votre ordinateur la génère lui-même. Soit l'adresse est attribuée manuellement (pour qu'elle soit courte et donc plus facile à taper).

Pour générer une adresse IPv6, certains systèmes comme Windows 7 tirent des nombres au hasard. D'autres, comme Windows XP, se basent sur l'adresse MAC de la carte réseau : ils changent d'état le 7ème bit, insèrent FFFE en plein milieu et collent le tout après FE80::.
On ne peut donc pas communiquer avec des hôtes éloignés en utilisant les adresses de lien local. Pour aller sur Internet, nous utiliserons des adresses globales.

Les adresses globales

Les adresses IPv6 utilisées sur Internet sont très structurées et hiérarchisées. Voir le tableau ci-dessous :

IANA	RIR	LIR	Client	Sous-réseau	Hôte
3 bits	20 bits	9 bits	16 bits	16 bits	64 bits

L'IANA est l'organisme qui gère les adresses IP sur Internet. Il a décidé que les adresses IPv6 utilisables sur Internet commenceraient par 2000::/3, puis il donne au RIR des valeurs sur 20 bits pour différentes zones géographiques. Chaque RIR donne ensuite aux LIR des valeurs pour chacun d'entre eux, qui eux-mêmes vont distribuer des valeurs aux clients, qui vont... etc.
L'IANA, c'est le chef. Il existe différents RIR pour différentes zones géographiques : l'ARIN pour l'Amérique du Nord, l'AfriNIC pour l'Afrique, *l'APNIC pour l'extrême-orient et l'Océanie,* etc.
Les LIR, ce sont les fournisseurs d'accès à Internet et les très grosses entreprises.
Ensuite, chacune de ces entreprises dispose en théorie de 65536 adresses pour ses clients.

Les adresses particulières

En dehors des adresses de lien local et globales, il existe aussi quelques adresses particulières à connaitre.

- **Les adresses courtes**

Celles-là sont appréciées pour leur facilité d'écriture. On trouve 2 adresses particulièrement courtes :

- ::1 : c'est l'adresse de la boucle locale (loopback). C'est l'équivalent de 127.0.0.1 en IPv4.
- :: (ou ::0) : c'est l'adresse que prend votre carte réseau avant de s'attribuer une adresse. Quand votre machine envoie une demande d'adresse au démarrage, elle le fait sous l'adresse ::.

- **Les adresses de site local**

Ces adresses sont attribuées au sein d'un site mais ne sont pas accessibles depuis le réseau public (comme les adresses privées en IPv4). Elles commencent par FEC0::/10 et sont structurées de la manière suivante :

10 bits	54 bits	64 bits
1111 1110 11	identifiant du sous-réseau	identifiant de l'hôte

Ces adresses peuvent être routées (elles peuvent passer des routeurs) dans le site local, mais pas au-delà.

- **Les adresses multicast**

Elles commencent par FF00::/8 et servent à désigner et gérer des groupes d'hôtes. Une adresse IPv6 qui commence par FF ne désigne pas un hôte.
Contrairement à IPv4, en IPv6, il n'existe pas d'adresse de broadcast !

- **Les adresses d'encapsulation**

IPv6 est compatible avec IPv4. On peut s'adresser à une adresse IPv4 même si on a juste une adresse IPv6. Comment faire alors pour désigner une adresse IPv4 en IPv6 ? En la représentant de cette manière :

10 octets	2 octets	4 octets
Que des zéros	FFFF(16)	L'adresse IPv4

Exemple

Adresse IPv4	Adresse IPv6 d'encapsulation
42.13.37.42	::FFFF:42.13.37.42
192.168.2.1	::FFFF:192.168.2.1

3.5. Comparaison entre IPv4 et IPv6

IPv6 encode les adresses sur 128 bits au lieu de 32 bits. Les adresses IPv4 ont une longueur de 32 bits et sont exprimées en notation décimale avec des points de séparation. Les adresses IPv6 ont une longueur de 128 bits et constituent un identifiant pour une interface ou un ensemble d'interfaces. Les adresses IPv6 sont affectées à des interfaces et non à des nœuds. Dans la mesure où chaque interface appartient à un nœud unique, toutes les adresses d'unicast attribuées aux interfaces du nœud peuvent être utilisées comme identifiant du nœud. Les adresses IPv6 sont exprimées au format hexadécimal avec des deux-points de séparation. Les champs IPv6 ont une longueur de 16 bits. Afin de faciliter la lecture des adresses, il est possible d'omettre les zéros de tête dans chaque champ. Le champ « 0003 » est écrit «3». La représentation abrégée IPv6 de 128 bits consiste en huit nombres de 16 bits, représentés par quatre chiffres hexadécimaux.